AIR COMMAND AND STAFF COLLEGE

DISTANCE LEARNING

AIR UNIVERSITY

# SPECIAL PURPOSE IT DERAILED: UNINTENDED CONSEQUENCES OF UNIVERSAL IT LAWS AND POLICIES

by

Peter L. Reichert, DAF



A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Proposal Adviser: Dr. Heather Marshall

Project Advisor: Dr. Andrew Niesiobedzki

Maxwell AFB, AL

October 2015

## Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

## Table of Contents

## List of Figures

## List of Tables

## PREFACE

In 2006 the Air Force initiated a campaign to consolidate local Information Technology (IT) networks into an enterprise architecture to reduce costs and to increase security. Leadership coined this as the "One Air Force, One Network" (1AF1N) initiative and feverishly set out to make this reality. Although well intended and applicable to the majority of Air Force networks there were unique networks incapable of participating without defeating the purpose of their existence. This was and still is especially true for the Research, Development, Test and Evaluation (RDT&E) community.

For example, the F-22 flight test program was based on a joint collaborative effort between the Air Force and Lockheed Corporation. To facilitate partnering between the Air Force and Lockheed, a joint IT network was established to link Air Force and contractor sites to seamlessly share program information. So when Air Force IT leadership tried to apply 1AF1N to the F-22 program network, IT leadership was pitted against the RDT&E community in a test of wills; essentially one program network versus 1AF1N each mutually exclusive. Unfortunately, because there were no exceptions to the 1AFAN initiative the F-22 program remained in a non-compliant stalemate for several years prioritizing program execution over compliance. This is but one example of many ongoing universal IT laws and policy challenges pitting RDT&E requirements against compliance.

This research project in large part was made possible through the support of my wife, daughters, friends and coworkers all who had the patients to bear with me through the many hours dedicated to the work. I would also like to thank all of my Air Command and Staff College professors and peers who each contributed in honing my critical thinking, writing, and research skills. Thank you all.

## ABSTRACT

The quantity of Information Technology (IT) has rapidly expanded within the federal government. As a result, the government spends in excess of $75 billion annually on IT.[2] This growth was unregulated with little thought of lifecycle management, modernization, security, configuration control, or centralized planning and control. Therefore, Congress began enacting laws and policies to establish governance over IT spending. These laws primarily target large data centers and enterprise IT with little exception for unique special purpose/platform IT. As such, all systems are required to comply with registration and reporting, data center level security controls, and other requirements imposing an impractical compliance burden on special purpose systems. For example, the average cost of compliance per system for the Certification and Accreditation (C&A) is $78,000 per system initially and $21,000 annually thereafter.[8] Thus, just taking into account the C&A costs, a conclusion can be made that for smaller systems, compliance costs may exceed the value and functional mission benefit of the system.

To explore the issue a problem/solution framework was used to define special purpose IT, identify key laws and policies, address intent, ascertain the level of previous research, assess impacts, and provide recommendations. In discovery, little research has been completed on the subject and to some extent concessions are being made for special purpose IT. However, there is room for improvement by tailoring policies based on results versus scorecards, drawing a distinction between IT enabled scientific equipment and traditional IT, increasing exceptions, establishing a DoD IT governance Research, Development, Test and Evaluation (RDT&E) mission area, and reassess what needs to be registered and reported. In summary; if the cost of compliance exceeds the system's value or benefit, compliance requirements should be challenged.

# INTRODUCTION

*Technology is dominated by two types of people: those who understand what they do not manage, and those who manage what they do not understand.*[1]

*Archibald Putt*

## *Overview of the Study*

Ever since Information Technology (IT) has come of age in the late 1980's, policy makers have struggled to govern the procurement, protection and use of this technology. Complicating matters, IT has evolved from a desktop office automation computing environment and now permeates as a force multiplier in all aspects of the Department of Defense (DoD) mission in the form of non-desktop or special purpose IT systems. For example, the same computer we use to check email and write reports can be used to operate milling machines or used to collect test data from an aircraft. In other words, special purpose IT systems are not those used for office automation and are typically not connected to the Internet. Rather they are dedicated to a specific function such as monitoring controls in an industrial plant, used to generate and display information in a control room such as what NASA uses during space missions, or to operate a Magnetic Resonance Imaging (MRI) machine in a hospital. This is only a small fraction of the many special purpose IT systems used throughout society. However, for the most part IT policy and governance fails to recognize the uniqueness of special purpose IT. This is especially true within DoD's Research, Development, Test and Evaluation (RDT&E) mission. The RDT&E mission of testing future weapon systems and capabilities often requires special purpose IT capabilities to accomplish the mission. Thus, by the very nature of special purpose IT being unique makes compliance with generic IT policies and laws difficult if not impossible.

To explore the issue in depth, this paper focuses on differentiating desktop and non-desktop special purpose IT uses and how universal IT laws and policies are inept and in some cases counterproductive in achieving the intent of IT laws and policy. The research then focuses on what might be done to address IT law and policy intent relative to special purpose IT without impacting the mission of those unique IT requirements.

***The Nature of the Problem***

From the inception of computer networking that interlinked office computers to one another and ultimately across the Internet as a means of communication and information sharing in the 1990's, the quantity of IT computer systems has rapidly expanded within the federal government and DoD. As a result the federal government currently spends in excess of $75 billion annually on IT.[2] This growth was unregulated with little or no thought for lifecycle management, modernization, and configuration control or centralized planning. Additionally, many of these systems have been designed without security in mind putting the hosted information and capabilities at risk. Furthermore, with the advent of networking, leaders soon realized that as systems began to interconnect, the system of systems would be difficult to manage without centralized control. As a result, Congress began enacting broad sweeping laws and policies in an attempt to establish control over federal government IT spending and to enforce cybersecurity. In 1996 Congress enacted the Information Technology Management Reform Act as a first attempt to establish governance and improve the management of government IT systems.[3] Then in 2002, Public Law 107-347 Federal Information Security Management Act was established to mandate cybersecurity baselines be established for all IT systems and thereafter validated annually.[4] Later, Public Law 112-81 National Defense Authorization Act for Fiscal Year 2012 refined IT financial governance and reporting

requirements.[5] These laws are broad in scope and primarily target large data centers as depicted in figure-1 below and enterprise IT systems such as *HealthCare.gov* with little or no exception for special purpose IT performing unique functions. The perceived need for IT governance is so pervasive that according to a congressional research report, there are more than 50 laws related to cybersecurity alone.[6]

Figure 1: FBI Data Center at the Criminal Justice Information Services Division[7]

***Purpose of the Study***

Because there are little or no exceptions for special purpose IT, all systems are required to comply with national registration and reporting, data center level security controls, and other bureaucratic requirements. The purpose of this study is to examine the compliance burden imposed on organizations that rely on special purpose IT. First, by exploring implementation and sustainment costs associated with compliance. For example, the average cost of compliance per system for just the certification and accreditation aspect is $78,000 per system initially and then $21,000 annually thereafter for required systems testing and validation.[8] This one compliance cost alone may exceed the procurement cost of the hardware and software of the

system not to mention the functional value or the purpose the system. For example, in simplistic terms, computer systems are used all across DoD as customer check-in kiosks to automate and replace sign-in sheets or manual "take a number" systems you might find in a deli. The automated kiosk provides a little more capability but still only really performs the function of the sign-in sheet. If just taking into account the procurement cost with a life expectancy of six years the daily cost to operate would be less than 50 cents a day. A little more than a sign-in sheet but with the added capability still a value. However, when you add the thousands of dollars a year for the certification and accreditation costs the benefit is far less than the cost to operate; time to go back to a spreadsheet. Therefore, in just taking into account the certification and accreditation costs a conclusion can begin to be drawn that for smaller systems compliance costs may exceed the functional benefit the system provides to the mission. Furthermore, the disproportionate compliance requirements may unnecessarily increase overall program costs, thereby ultimately defeating cost reductions goals intended by the laws and policies. Thus, the purpose of this study is to review to what extent compliance requirements, relative to RDT&E special purpose IT, bring value versus impair utility.

***Research Question***

When people think of IT or computers they tend to gravitate to the typical desktop office automation environment, large data centers, or computer clouds. Rightfully so, this use of IT is by far the most prevalent and visible. So it is only natural for governance bodies to focus laws and policies on this majority. However, the minority applications of IT used in a myriad of special functions beyond office automation often goes unseen as policy makers address the issues of the greater IT world. Therefore, IT laws and policies tend to be general in nature to target macro level concerns. Based on this, the research question for this study is how effective

and more importantly, how economical are federal and DoD IT laws and policies when applied to special purpose IT Computer Systems (*see Definition of Terms in appendix A for a description of "effective and economical" relative to this study*).

### *Definition of Terms*

See Appendix A

### *Research Methodology*

A problem/solution framework has been used to conduct and document this work. The paper first explores the problem associated with generic overarching IT laws and agency policies and how they affect special purpose IT. The paper then introduces applicable laws, policies and compliance requirements associated with the laws and policies. Next, the study explores the intent of compliance requirements from a financial and cybersecurity perspective. Moving on, a review of governance requirement goals will be contrasted with mission execution challenges to frame the dilemma. This aspect will require a notional cost benefit analysis based on average compliance costs and the functional benefit of special purpose IT to contrast and balance compliance requirements and mission execution. Finally, the paper summarizes the subject and reemphasizes the salient points and reviews the recommended way forward.

## LITERATURE REVIEW

### *Introduction*

To understand the effectiveness of enterprise IT governance laws and policies on special purpose IT systems an understanding of what constitutes special purpose IT was researched. Additionally, a review of IT law and policy was needed to assess compliance requirements in order to understand dichotomy between special purpose IT compliance and function. Lastly, research was conducted to determine the extent of other scholarly work on the subject matter.

Research results indicated there is a distinction between traditional and non-tradition special purpose IT and that many foundational laws and policies fail to take into account the uniqueness of special purpose IT. Moreover, research showed there was little scholarly material addressing the subject matter especially relating to RDT&E special purpose systems, which is at the center of this research.



### *Background*

Computers have become an integral component for almost every military function; desktop computers are used daily to write reports, generate presentations and spreadsheets, manage information and processes, communicate via email, just to mention a few. These computers are networked to large data centers which host files, applications, databases, and web servers. These uses are commonly referred to as defense business systems. Computers also have become indispensable in other aspects of the mission. For example, computers are embedded in weapons systems, integrated into medical instruments, used to monitor and provide access to secure environments, embedded in industrial control systems, and used to facilitate RDT&E of military weapon systems. These latter special purpose IT uses are in some cases also known as

platform IT (PIT). As an example, figure-1 depicts an IT enabled instrumentation telemetry ground station used to analyze and monitor test aircraft parameters via radio frequency link.

Figure 2: iNET Instrumentation Telemetry Ground Station[9]

With so many uses of computers in countless settings and situations the military range of IT is so broad in scope that no one policy could possibly address the nuances and applicability across the entire range of IT. However, many current federal and DoD IT laws and policies, geared primarily towards the traditional desktop and data center computer environments or defense business systems, do just that by not taking into account the uniqueness of special purpose IT**.** The Office of Management and Budget (OMB), for example, defines a data center as a "closet, room, floor or building for the storage, management, and dissemination of data and information."[10] By this broad definition any room with a computer could be defined as a data center. Moreover, on 18 August 2013 the Air Force issued a memorandum mandating registration of computer systems into a compliance tracking database to comply with Public Law 112-81. The law additionally prohibits the expenditure of funds for IT systems unless approved by the DoD CIO and, because there is no differentiation between traditional and special purpose IT, the law applies equally to all systems.[11] Based on OMBs liberal definition and Public Law

112-81, special purpose IT computer systems are expected to comply with resource intensive data center policy compliance requirements intended for multimillion dollar data centers; by doing so these laws and policies impose an excessive operational burden on small special purpose IT systems.

Conversely however, it can be argued a computer, regardless of function is a financial investment and contains cyber risks that must be managed with the same rigor as applied to all others. Therefore, policy mandating security configuration and financial management is applicable across the entire spectrum of IT. Rightfully so, all computer utilization should address security concerns and financial cost benefit analysis review. However, if policies are not adapted for special purpose IT computer systems the resources and costs necessary to maintain compliance will either be unattainable or outweigh the utility of the system ultimately imposing an undue burden on organizations whose missions rely on special purpose IT. In some cases this in turn drives bad organizational behavior manifested through willful lack of reporting and noncompliance.



***What Constitutes Special Purpose IT***

The literature review focused on differentiating traditional and non-traditional special purpose IT, in some cases known as Platform IT (PIT). DoD defines PIT as "IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems."[12] DoD goes on to specifically cite, as an example, "equipment used in the research and development of weapons systems."[13] Examples of RDT&E PIT include computers connected to weapons systems to calibrate and prepare test instrumentations sensors systems, simulators and stimulators needed to pre-run and predict test events, and data acquisition and analysis systems. By this definition a clear distinction is drawn

between traditional defense business IT systems, PIT and more specifically RDT&E PIT thereby, acknowledging the unique aspect of PIT. Furthermore, "PIT systems that are stand-alone must be authorized to operate, but assigned security control sets may be tailored as appropriate with the approval of the AO (e.g., network-related controls may be eliminated)."[14] The keyword in this quote is "tailored," meaning DoD has recognized to some extent not all IT is equal and those that may be stand-alone, not connected to an external network nor share information with a externally connected network do not need their cybersecurity posture scrutinized as much as those that are connected; a step in the right direction.

***Laws, Policies, and Compliance Requirements***

As mentioned above the federal government has good reason to exact governance over IT procurement, management and disposition in order to bring into control wasteful spending and cyber surety. To understand this, it is as simple as reviewing recent news trends related to botched IT project implementation, IT security breaches relating to personal identifiable information, and other critical information being exfiltrated by national and international hacking efforts. In the most recent and alarming event OPM in April of 2015 discovered hackers were able to access and retrieve personnel data from an OPM database. Later, "in early June 2015, OPM discovered that additional information had been compromised: including background investigation records of current, former, and prospective Federal employees and contractors. OPM and the interagency incident response team have concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen … and approximately 5.6 million include fingerprints."[15] However one thing to note, this hack was related to a major federal IT business system and not special purpose IT.

So with these serious events occurring, the first challenge of governance is to identify and document all current federal IT systems by documenting their existence, purpose, security configuration and status, and sustainment funding requirements to include labor and material. In essence in order to govern something you need to know what you have. The Air Force's primary tool to accomplish this is the Enterprise Information Technology Data Repository (EITDR). EITDR is a comprehensive data repository where Air Force system owners host applicable system information as mandated by many federal laws as defined below.

> The Air Force database of record for registering all systems and applications as required by public law and DoD directives. Registration in the EITDR is mandatory for all systems and applications developed by the Air Force, or for which the Air Force is the lead agency, or that requires connection to the AF-GIG. The EITDR is also the database of record for IT statutory and regulatory compliance. The repository contains compliance data for Information Assurance (IA), Internet Protocol version 6 (Ipv6), Public Key Enabling (PKE), Clinger-Cohen Act, etc. It is the primary data source for Federal Information Security Management Act (FISMA) reporting and the principal vehicle for gathering and storing system and application data to support planned and ad hoc data calls. The EITDR contains information about program management; system and application interfaces; networthiness; funding; Capital Investment Reports (CIRs) and other supporting data to facilitate IT portfolio management.[16]

As can be seen by the above definition, EITDR is a one stop activity whereby the registration and reporting requirements are significant and time consuming. Moreover, as noted by regulation, "[a]ll systems on which AF dollars are spent must be registered in EITDR, the official Air Force registration vehicle for ISs, with the exception of those identified by other policy (e.g. SPACE, Special Access Programs/Special Access Required, Joint, etc), to be registered in another registration vehicle."[17] The take away, no exceptions are made for size, dollar threshold, use, network connectivity, or categories such as RDT&E or special purpose IT. When a system is entered in the EITDR it is not only a matter of initial registration, it is also matter sustaining currency of the information for as long as the IT system is in use. Additionally, system managers must conduct annual validations, and responding to a litany of constant higher headquarters data inquiries.

Once legacy systems are registered, the task advances to managing sustainment costs. Laws and policies control this through leadership review and requirement verification, consolidation and regionalization, conversion to commercially available applications and services, and standardization of capabilities. The major forcing function for consolidation is the Federal Data Center Consolidation Initiative (FDCCI). FDCCI was established by the Federal CIO Vivek Kundra on 26 February 2010 to curb and govern federal data center expansion. In little more than a decade "Federal data centers grew from 432 in I998 to more than 1,100 in 2009. This growth in redundant infrastructure investments is costly, inefficient, unsustainable, and has a significant impact on energy consumption."[18] Being of serious concern, FDCCI was later codified as Public Law 113-291, the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015. The Air Force's response to FDCCI was the establishment of an IT Governance Executive Board (ITGEB) who would oversee and authorize all Air Force installation data centers; "ITGEB-approved data centers are the only authorized data centers for the AF to employ application hosting and provisioning of private cloud services."[19] The ITGEB defined the installation primary data center as an Installation Processing Node (IPN) of which there can only be one. All other data centers on an installation must fall into the category of a Special Purpose Processing Node (SPPN) of which must be physically incapable of consolidating into the IPN.

In parallel to managing costs, emphasis is made to ensure systems and the information hosted on the systems is secure. The primary law governing system security is the Federal Information Systems Management Act (FISMA) of 2002 with the intent to "provide a comprehensive framework for ensuring the effectiveness of information security controls over

information resources that support Federal operations and assets."[20] DoD describes and categorizes risk to include PIT systems in the following figure.

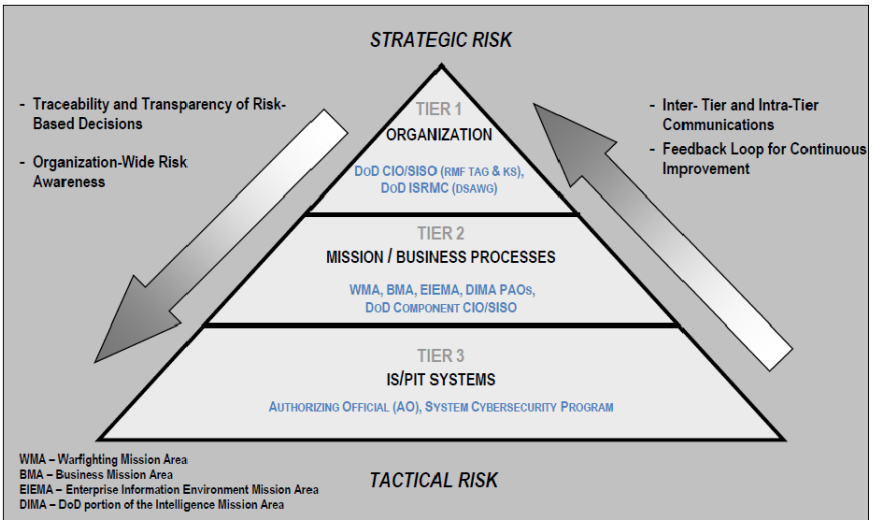


Figure 3: DoD Risk Management Framework Governance[21]

Air Force compliance with FISMA is managed by Air Force Instruction (AFI) 33-200 "Air Force Cybersecurity Program Management." AFI 33-200 governs measures needed to "ensure the confidentiality, integrity, and availability (CIA) of AF IT and the information they process. This AFI ensures the use of appropriate levels of protection against threats and vulnerabilities; helps prevent denial of service, corruption and compromise of information, and potential fraud, waste, and abuse of government resources."[22]

The cybersecurity compliance requirements established by regulation, although necessary, are daunting to achieve and maintain. To such an extent the federal government according to an OMB Circular A-11 report, found "[a]gencies reported over 60,000 Full Time Equivalent (FTE) positions with primarily security-related duties. At an average cost of $159,000 per FTE, the cost for these employees exceeds $10 billion."[23] What makes cybersecurity compliance so daunting is the many aspects that must be addressed. The first aspect of

cybersecurity mandates system administrators must be certified commensurate with the level of the system as designated by DoD 8570.01-M as highlighted in Figure-2.

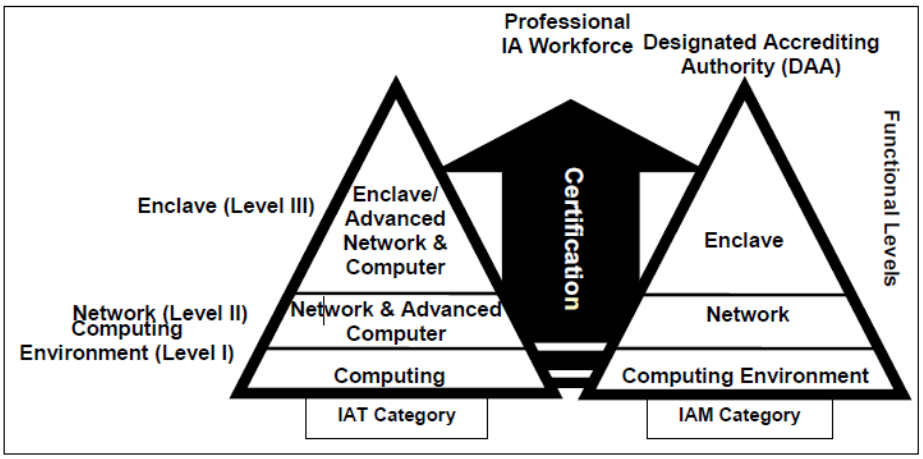


Figure 4: Overview of Basic IA Workforce Structure[24]

These certifications are costly, time consuming, and difficult to attain. Each level requires specific training and testing to attain initial certification and then annual continuously learning requirements to sustain certification. Aside from administrative responsibilities the system hardware and software must be also approved by being listed on an authorized approved product list or specifically evaluated and approved by an authorized Authorizing Official (AO) formally known as Designated Approving/Accrediting Authorities (DAA). These AOs typically reside at an agency or major command level and due to workloads have limited accessibility and response times are often sluggish. This approved hardware and software must then be configured to meet standards. System configuration standards are evaluated based on compliance with information assurance controls. Information Assurance (IA) controls are configuration items or security elements that specifically address configuration features of the system. Within the federal government IA controls map to the National Institute of Standards and Technology (NIST) special publication 800-53. The NIST publication identifies 17 families of controls as identified in table-1.

| CLASS | FAMILY | IDENTIFIER |
|---|---|---|
| Management | Risk Assessment | RA |
| Management | Planning | PL |
| Management | System and Services Acquisition | SA |
| Management | Certification, Accreditation, and Security Assessments | CA |
| Operational | Personnel Security | PS |
| Operational | Physical and Environmental Protection | PE |
| Operational | Contingency Planning | CP |
| Operational | Configuration Management | CM |
| Operational | Maintenance | MA |
| Operational | System and Information Integrity | SA |
| Operational | Media Protection | MP |
| Operational | Incident Response | IR |
| Operational | Awareness and Training | AT |
| Technical | Identification and Authentication | IA |
| Technical | Access Control | AC |
| Technical | Audit and Accountability | AU |
| Technical | System and Communications Protection | SC |

Table 1: NIST 800-53 Security Control Classes, Families, and Identifiers[25]

Each familiy of controls have numerous specific controls associated with them for a total of over 800 individual IA control configuration items. As mentioned earlier, not all IA controls are applicable to every system depnding on the function and classification of the system.

However, the IA effort does not stop with proper application of IA controls. Based on technology evolution IT hardware and software versions have a shelf life. As new vulnerabilities are discovered system hardware and software must be refreshed address the new risks. The Air Force addresses new vulnerabilities through a "cyber order flow process,"[26] whereby Time Complaince Network Orders (TCNO), Maintenance Task Orders (MTO), and Cyber Tasking Orders (CTO) are distributed throughout the Air Force for systems to be updated and patched to counter known vulnerabilities. These notices are weekly if not daily events and drive a great deal of overhead on systems management. For example, in 2014 365 TCNO's were distributed and as of the end of September 2015 there have been 337 distributed within 2015.[27] Lastly,

Defense Information Systems Agency (DISA) develops and maintains Security Technical Implementation Guides (STIG) for mandatory implementation on all DoD systems. DISA STIGs provide hardware and software configuration guidance to further secure systems from malicious computer attack as an enhancement to NIST IA controls.

To ensure compliance with all of the above systems are inspected or under threat of inspection on a regular basis to include local information assurance assessment program, unit effectiveness, operational readiness, and Cyber Command rediness inpections, to name a few. So to put this into perspective from one end of the spectrum; a user of a single simple computer connected to a metal lathe or milling machine who has no IT skills must take the time to become certified, register the system, account for all financial data, and sustain that computer in the EITDR and ensure all applicable IA controls are addressed, STIGs applied, and patches maintained in accordance with TCNOs, MTOs, CTOs, and other mandates.



***Previous Research***

For the most part this research charts new ground. Acknowledgement of issues relating to RDT&E is touched upon in non-scholarly trade publications at an editorial level but no scholarly research has been uncovered addressing IT law and policy impacts relating to RDT&E special purpose IT. However, by DoD recently acknowledging PIT in "DoDI 8500.1" as mentioned earlier in the tailoring of IA controls based on PIT functionality, leadership for at least the cyber surety aspect of governance is realizing not all IT is of the same ilk. Further indication of PIT being recognized as unique can be found in a memorandum from Air Force Material Command (AFMC)/A6/7 whereby it clarifies RDT&E PIT by stating "due to the uniqueness of AFMC's RDT&E mission … we felt it is necessary to provide clarification regarding what types of purchases/equipment fall under FDCCI. Generally, if an organization is using IT equipment

to perform real-time data acquisition or which is embedded into a larger RDT&E system, it is not considered a data center and not within the scope of the FDCCI."[28]

## ANALYSIS

### *Crux of the Situation*

At the core of this analysis a struggle exists between the value of utility versus compliance, in other words the cost benefit analysis. There is no argument as to the necessity to maintain a certain level of governance for all IT systems but when the compliance burden begins to far outweigh a system's usefulness in effort and cost, one of four things will occur. Either, the IT system will be brought into compliance, abandoned resulting in lost productivity, nefarious workarounds or shadow operations will be established, or systems will blatantly be operated in a non-compliant configuration. These latter options are especially true and tempting in these times of scarce resources. When the temptation is to operate out of compliance, undue risk is likely being accepted from a cybersecurity perspective and any attempts to achieve greater efficiency through standards and consolidation are lost defeating the intent of governance. If brute force is applied to facilitate compliance, labor and funding resources will be diverted from potentially other critical mission needs or overall programs costs will be increased detrimentally impacting operations; again defeating the intent of governance. Proportionally, as the compliance burden decreases the more likely systems will be brought into compliance resulting in restored operations and more importantly improved security and efficient operations will be achieved as intended by governance. So what is needed to strike a balance between the two objectives of compliance and utility.

Aside from the cost benefit of compliance another issues looms in that some special purpose IT systems are so specialized complete compliance is not possible without impairing or completely destroying the systems function. For example, the software application installed on the system to perform the specific function may have been software hard coded specifically to

the IT system's Operating System (OS) software at the time of installation such as Microsoft Windows XP. Then, when Microsoft releases a new OS to overcome vulnerabilities of XP compliance requirements will mandate the installation of the new OS. However, if the new OS were installed the legacy hard coded application would likely cease to function since it was not coded to run with the new OS software until the organization spends the money to have the legacy application recoded to work with the new OS. This is no different from what people experience at home with their personal computers when the OS is upgraded and they find out some previous applications no longer work. The difference in some cases is that the software application on the special purpose IT system may be one of a kind because of the RDT&E mission requirement and to rewrite the application to be compatible with the new OS will cost $100,000 (based on a real RDT&E example). At first this cost seems extraordinary, but when taken in perspective of being one of a kind and as mentioned earlier the cost of a FTE being in some cases as much as $159,000 annually, it is easy to see this reality. Therefore, in the case of a system only performing a single specific function while not connected to any other computer or network, it would not be in the interest of the government to mandate compliance at such an exorbitant cost when it adds little or no value. Rather it would be better to mitigate the risk by some other fashion; for example, increasing scrutiny of files that are transferred to or from the RDT&E system to ensure no malware can be induced into the system to take advantage of the expired OS. In this case a compliant buffer system could be used as an intermediary device to ensure the transferred files are clean from malware as they transition. Moreover, as it currently stands, senior officials too far removed at a Major Command (MAJCOM) level might have difficulty understanding this nuance of the system and therefore may not be best suited to make these risk determinations. Bottom line; the intent of compliance is it just not an action to go

through the motions as directed from above, rather compliance in some cases needs to be explored more analytically to take into consideration of all variables associated with a system. This is especially true and relative to the RDT&E special purpose IT environment.

***Intent of Laws and Policies***

So clearly laws and policies are intended for major IT systems and data centers, especially those connected to the Internet; but how far does the intent extend to the other end of the spectrum. Is the intent of laws and polices meant for small IT systems/computers and special purpose IT and to what extent. To answer this, when OMB in 2011 modified the definition of a data center from "any room used for the purpose of processing or storing data that is larger than 500 square feet, is used for processing or storing data, and meets stringent availability requirements"[29] to the current definition of "a closet, room, floor or building for the storage, management, and dissemination of data and information"[30] certainly expands the envelope of what now is a data center to include any room with a computer in it. Furthermore, although DoD makes some cybersecurity concessions for lower level tiered IT, all IT regardless of size or use is intended to comply with laws and policies virtually without exception. As such, how practical is this liberal compliance approach when it comes to RDT&E special purpose IT. Moreover, based on the above and OMB's new data definition, this liberal compliance construct not only puts an additional burden at the system level on the military installation were it resides, but also adds significant workload to the compliance approval chain by now having to address the new magnitude of effort primarily as a result of the more liberal definition. For example, "[u]nder the first definition, OMB identified 2,094 data centers in July 2010. Using the new definition from October 2011, OMB estimated that there were a total of 3,133 federal data centers in December

2011."[31] This greater than 1,000 increase in identified data centers added significantly to the governance workload of all stake holders from the system owner to the approving authority.

With intent established that all systems must meet compliance standards then to what extent do DoD and the Air Force have to identify those standards to make them commensurate with the level and value of the PIT system. As mentioned earlier DoD, has already produced tailored IA controls for PIT systems thereby DoD has the authority to further tailor and delegate cybersecurity compliance requirements. From a cybersecurity perspective, one of the key intents of DoD policy is to achieve reciprocity across all of DoD and the rest of the federal government. According to DoD, "reciprocity is best achieved through transparency (i.e., making sufficient evidence regarding the security posture of an IS or PIT system available, so that an AO from another organization can use that evidence to make credible, risk-based decisions regarding the acceptance and use of that system or the information it processes, stores, or transmits). DoD Components must share security authorization packages with affected information owners (IOs) or stewards and interconnected ISOs to support cybersecurity reciprocity,"[32] again a large step in the right direction to prevent redundant and wasteful efforts. By understanding intent, governance boards at all levels and AOs are better equipped to ensure any process customizations they establish will provide the desired results at higher levels.

***Conclusion***

This study explored how effective and more importantly, how economical are federal and DoD IT laws and policies when applied to special purpose IT Computer Systems. The research drew a distinction between traditional office automation and special purpose IT. From there the study delved into the nature of the problem by identifying the uniqueness of RDT&E PIT systems and how laws and policies, although have provided some concessions for RDT&E, are

for the most part still focused on the majority of more traditional IT environments which results in ineffectiveness and non-compliance.

What was discovered is that without a doubt it is in the best interest of the government to provide governance for all IT systems to ensure cyber surety and financial prudence. However, IT law and policy requirements mainly targeting large federal and DoD IT systems are in some cases impractical when applied to smaller more special purpose IT systems. This is especially true relative to the DoD and Air Force RDT&E mission. If IT governance fails to adequately adapt requirements commensurate with the lesser value and scope of these IT systems, there will either be a significant increase in the cost of RDT&E activities to attain compliance or the RDT&E community will be compelled, due to insufficient resources, to operate outside of compliance.

As an indirect consequence of being unable to comply, the potential exists for systems owners to completely disregard any cyber surety fortification or thought of financial efficiency for fear of being subjected to unattainable enterprise requirements. As such, if no attempt is made at compliance, these systems will be at risk contrary to the intent of what laws and policies where setting out to achieve. Therefore, this research suggests IT governance boards should take the time to recognize the burden being placed on these smaller specialized IT systems and adapt requirements accordingly. By doing so, the more likely the end result of increased cyber surety, cost savings, and efficiency for all IT systems regardless of function or scope will be achieved.

To truly understand the burden and effectiveness of compliance, compliance cost information must be collected for all levels of IT. Once the information is gathered a business case analysis must be completed to weigh compliance against system utility and value. Where compliance costs exceed value would be the target to reassess compliance requirements for those

types of systems. For those systems where compliance costs may exceed value, recommendations have been provided on how to balance compliance against RDT&E operations by limiting financial reporting and moving cybersecurity decisions closer to onsite leadership. In doing so, the leadership at this level will be more cognizant of the system and mission in order to mitigate and manage compliance requirements against available resources.

In summation, research indicates there is room for improvement within current IT governance laws and policies to account for the practical governance of special purpose IT systems without losing sight of enterprise level goals. This is especially true relative to IT management cost reductions where in certain cases it costs more to attain and maintain compliance than the original procurement cost of the system or the value the system adds to the mission. When these costs are inverted it is time to reassess requirements and processes for a better way to achieve end results. As mentioned earlier when the United States federal government is spending greater than $75 billion annually on IT costs and $10 billion or 13% of the total cost is dedicated to the labor needed to address cybersecurity alone something is out of balance.

***Recommendation***

At a macro level it is time for governance boards to refocus of what is trying to be achieved; generally speaking cost reductions and increased cyber surety focusing primarily on enterprise office automation business systems. Assumptions should not be made that closures of data centers and consolidation of IT systems necessarily leads to cost savings without actually tracking real, not cost avoidance, budget reductions. Additionally, assumptions should not be made that IT systems are more secure by the number of systems being certified and accredited

without corresponding reductions in the number of cyber incidents being reported. In other words, focus on end results not bureaucratic scorecard metrics.

At a federal level OMB should redefine what constitutes an IT system and data center by drawing a clear distinction between office automation business systems, PIT, and computer aided tools. Based on these new definitions, exclusions should be made for IT systems that might be now out of the scope of law and policy intent. For instance, OMB's definition of a data center already excludes telephone switches and communication closets even though these areas potentially contain IT systems by stating "[excluding facilities exclusively devoted to communications and network equipment (e.g., telephone exchanges and telecommunications rooms)]."[33] Based on this it seems reasonable to further define and provide some additional exclusion for RDT&E systems as being out of scope for the purpose of enterprise governance or better yet move governance responsibility to a more closely aligned discipline such as the scientific community. For example, the telemetry ground station as earlier in the study is more closely related to a piece of scientific equipment than it is to IT. And as stated earlier this is but one of many types of RDT&E special purpose IT functions. Therefore, when these systems more closely resemble scientific equipment then maybe they would be better suited being governed through the scientific community rather than IT.

At a DoD level, the first step in addressing the problem is through formal recognition of the RDT&E mission. All agencies within DoD conduct RDT&E and in many cases this mission crosses agency boundaries and in those cases there are interagency governance structures to address this subset of the DoD RDT&E mission. For example, "Major Range and Test Facility Base [MRTFB] is a set of test installations, facilities, and ranges which are regarded as 'national assets.' These assets are sized, operated, and maintained primarily for DoD test and evaluation

missions."[34] As such, "[i]n 1971, DoD recognized that large military test facilities represented national assets and were required to support development and deployment of U.S. warfighting capabilities. DoD established the MRTFB management concept to provide coordination among the major facilities, promote multi-Service use, reduce unnecessary duplication of assets and establish budgetary priorities at the Department level."[35] Not only is the MRTFB concept recognized by DoD it is also specifically addressed by public law 107-314. The law directs DoD to "establish within the Department of Defense … a Department of Defense Test Resource Management Center."[36] Furthermore, as part of the law, congress directs the Center to provide oversight of the MRTFB. However, even with this level of visibility as can be seen in figure-3, "DoD Cross-Mission Area Forum," nowhere in the structure is RDT&E or MRTFB addressed. As important as RDT&E is to the future DoD mission it is time to recognized RDT&E's unique mission in DoD's IT portfolio governance structure as a major mission area or subdomain.

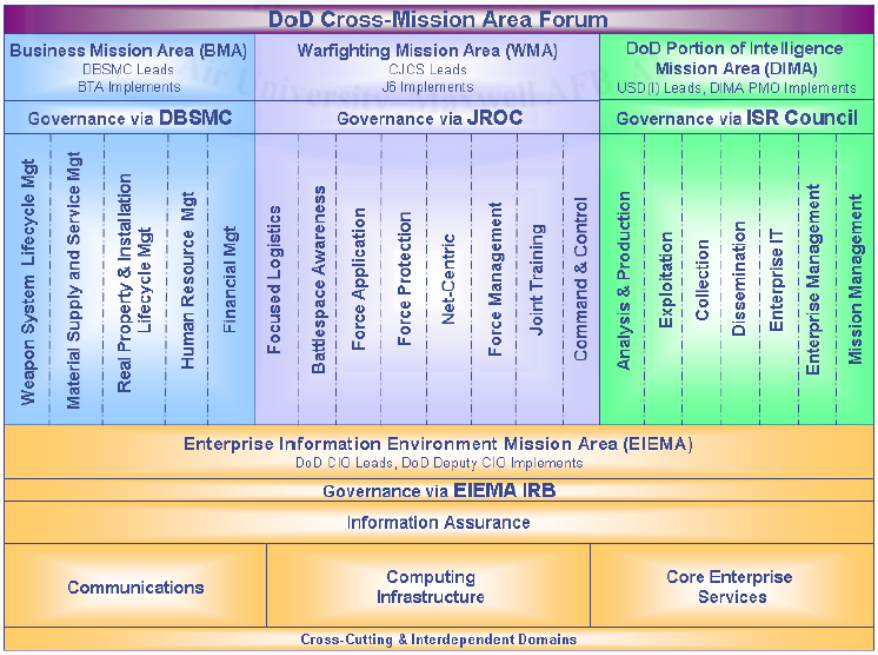


Figure 5: DoD IT Portfolio Governance Structure[37]

To acknowledge RDT&E, DoD should establish a RDT&E mission area within the IT portfolio governance structure. By doing so, DoD will eliminate IT governance complexities as a result of other mission area governance boards trying to provide RDT&E IT governance based on their mission area processes that are not suited for the uniqueness and agility required by RDT&E.

From an RDT&E PIT perspective DoD and Air Force need to continue to recognize the uniqueness of PIT systems by continuously seeking to streamline compliance measure. Focus needs to be cognizant of value of utility versus compliance cost. Compliance measures, without jeopardizing cybersecurity and financial management, must be proportionate to the utility, risk (threat plus vulnerability), scope, significance, and connectivity of the system. The greater these values, the greater level of scrutiny and compliance and conversely, the lesser the values, the less scrutiny. Bottom line, compliance costs should never come close to exceeding these values; if so overall intent has been lost.

DoD and Air Force policy makers in some cases seem to conceptually understand balancing value and compliance, for example tailoring IA controls but the focus is more on reduced effort versus trying to understand cost benefit analysis of compliance. In order to begin understanding cost of compliance, data will need to be collected from all levels of the compliance chain to get a factual and detailed understanding of the level of effort and cost being expensed towards compliance. For instance, have the system owners' track the hours they spend bringing the system into and maintaining compliance itemized by system registration, IA certification, STIGing, patching, gathering and reporting financial information, and responding to data calls in a given year. Collecting data will initially add to compliance cost and overhead but without this information there is no way to truly understand impacts. Once this factual

information is gathered a business case analysis can be conducted to get an understanding of how compliance might be missing the mark relative to some PIT systems. Then compliance might be adjusted accordingly to attain a more realistic outcome.

Based on the macro data of IA certification at $78,000 per system for initial certification, it is not too hard to summarize this one cost of compliance alone will exceed many small IT systems value of utility. One way to mitigate this unbalanced cost versus utility for smaller IT systems is to establish thresholds for non-networked small systems. A great threshold might be based on the system's complexity. Such as, the greater the complexity the higher in the chain of command the system owner must go for authorization; versus, the less complex then the lower the chain of command for authorization. Additionally, alternatives could be based on cost, importance to the mission, degree the systems has to communicate externally with other systems via file transfer, or a hybrid of the above. Then, for those systems below the threshold delegate authorization, reporting, and oversight back down to a military base installation level IA office. This should not be a far reach since DoD already recognizes the need for AOs to be cognizant of PIT systems and missions when DoD states "PIT expertise must be a factor in the selection and appointment of AOs responsible for authorizing PIT systems."[38] However, as it stands currently the Air Force has chosen not to delegate AOs below the MAJCOM level. To this extent the person at the MAJCOM level may have a level of cognizance for major PIT systems within their jurisdiction but little cognizance for minor instances. In these cases it would make sense to further delegate AO responsibility to installation level to ensure the AO has cognizance of what they are responsible for managing. Moving the AO responsibility closer to the mission ensures a greater understanding of the value of utility versus compliance not to mention ability to provide greater oversight of the cybersecurity posture of the system.

Lastly, the Air Force should reassess what types of IT systems need to be reported in the EITDR. If OMB and DoD redefine scope and intent, RDT&E PIT may no longer be applicable for reporting. Moreover, many RDT&E systems are usually part of a bigger specific program effort or weapon system whereby financial reporting is at a program level. For instance, Edwards AFB control rooms used by Joint Strike Fighter (JSF) are funded by the JSF program. If the Air Force where to report the JSF control rooms as an IT system in the EITDR a duplication of reporting is likely to occur since the JSF program is also obligated to report program financial data to DoD and congress to include funding spent on the control rooms. If financial data then were to be independently compiled it may appear JSF expenditures are more than actual costs. This could become critically detrimental for these high visibility programs which under constant political watch where every dollar being spent is heavily scrutinized by critics of the program.

## Endnotes

[1] Archibald Putt, *Putt's Law and the Successful Technocrat: How to Win in the Information Age*, April 2006.

[2] *IT Dashboard FY2015 Edition.* https://itdashboard.gov/portfolios.

[3] *Information Technology Management Reform Act of 1996.* Public Law 104-106. 104th Cong., 10 February 1996.

[4] *Federal Information Security Management Act of 2002.* Public Law 107-347. 107th Cong., 17 December 2002.

[5] *National Defense Authorization Act for Fiscal Year 2012.* Public Law 112-81. Cong., 112th. 31 December 2011.

[6] Eric A. Fischer, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, Congressional Research Service, 20 June 2013, ii.

[7] Federal Bureau of Investigation website, *Next Generation Identification: FBI Announces Biometric Suite's Full Operational Capability*, 23 September 2014, https://www.fbi.gov/news/stories/2014/september/fbi-announces-biometrics-suites-full-operational-capability/fbi-announces-biometrics-suites-full-operational-capability

[8] Office of Management and Budget. *Fiscal Year 2009 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002.* Pg. 14-15.

[9] Thomas Grace, Department of the Navy TAS Chief Engineer, *Telemetry of the Future*, briefing presentation, date and location unknown, slide 17.

[10] Steven VanRoekel, Federal Chief Information Officer Memorandum. *Implementation Guidance for the Federal Data Center Consolidation Initiative (FDCCI).* Office of management and Budget Washington D.C. 19 March 2012.

[11] Michael J. Basla, Lt Gen, USAF. *Air Force Guidance Memorandum to AFI 33-150, Management of Cyberspace Support Activities.* Department of the Air Force Washington D.C. 18 August 2013.

[12] Department of Defense Instruction DoDI 8500.1, *Cybersecurity*, 14 March 2014, 58.

[13] Ibid., 39.

[14] Ibid.

[15] "Cybersecurity Resource Center," OPM.gov, U/S/ Office of Personnel Management, accessed 26 September 2015, https://www.opm.gov/cybersecurity

[16] Air Force Instruction (AFI) 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP),* 23 December 2008, 38.

[17] Ibid., 17.

[18] Vivek Kundra, first United States Federal Chief Information Officer March 2009 through August 2011, *Memorandum for Chief Information Officers: Federal Data Center Consolidation Initiative*, 26 February 2010.

[19] Air Force Instruction (AFI) 33-115, *Air Force Information Technology (IT) Service management*, 16 September 2014, 7.

[20] Public Law 107-347. *Federal Information Security Management Act of 2002,* Title III-Information Security, SEC. 301 § 3541. Purposes (1).

[21] Department of Defense Instruction (DoDI) 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT),* 12 March 2014, 14.

[22] Air Force Instruction (AFI) 33-200, *Air Force Cybersecurity Program Management*, 31 August 2015,6.

[23] OMB, *2009 Report to Congress on the Implementation of FISMA*, 11.

[24] Department of Defense (DoD) 8570.01-M, *Information Assurance Workforce Improvement Program*, 24 January 2012, 19.

[25] National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005, 6.

[26] Air Force Instruction (AFI) 10-1701, *Command and Control (C2) for Cyberspace Operations*, 5 March 2014, 4.

[27] 33d Network Warfare Squadron, *Advisory List*, accessed on 24 September 2015, https://33nws.lackland.af.mil/advisories/advisory-list.asp.

[28] Terry G. Edwards SES DAF, AFMC/A6/7 Director of Communications Installations and Mission Support, *Memorandum for ALHQCTR/CC/CL, ALHQSTAFF, AL INST/CC/CL: Guidance on Approval of Obligation of Funds for Research, Development, Test and Evaluation (RDT&E)*, 11 September 2104.

[29] United States Government Accountability Office Report to Congressional Requestors, report GAO-14-713, *Data Center Consolidation: Reporting Can Be Improved to Reflect Substantial Planned Savings*, September 2014, 6.

[30] Ibid.

[31] GAO-14-713, *Data Center Consolidation*, 6.

[32] DoDI 8500.01, *Cybersecurity*, 30-31.

[33] GAO-14-713, *Data Center Consolidation*, 6.

[34] Global Security website, *Military*, "Major Range and Test Facility Base [MRTFB], accessed 10 October 2015, http://www.globalsecurity.org/military/facility/mrtfb.htm

[35] Ibid.

[36] Public Law 107-314, *Bob Stump National Authorization Act for Fiscal Year 2003*, 2 December 2002, 31.

[37] Air Force Instruction (AFI) 33-141, *Air Force Information Technology Portfolio Management and IT Investment Review*, 23 December 2008, 5.

[38] DoDI 8510.01, *RMF*, 10.

## Bibliography


33d Network Warfare Squadron official website, "Advisory List." Accessed on 24 September 2015. https://33nws.lackland.af.mil/advisories/advisory-list.asp.

Air Force Instruction (AFI) 10-1701. *Command and Control (C2) for Cyberspace Operations,* 5 March 2014.

Air Force Instruction (AFI) 33-115. *Air Force Information Technology (IT) Service Management,* 16 September 2014.

Air Force Instruction (AFI) 33-141. *Air Force Information Technology Portfolio Management and IT Investment Review,* 23 December 2008.

Air Force instruction (AFI) 33-200. *Air Force Cybersecurity Program Management,* 31 August 2015.

Air Force Instruction (AFI) 33-210. *Air Force Certification and Accreditation (C&A) Program (AFCAP),* 23 December 2008.

Basla, Michael J., Lt Gen, USAF. *Air Force Guidance Memorandum to AFI 33-150, Management of Cyberspace Support Activities.* Department of the Air Force Washington D.C. 18 August 2013.

Bob Stump National Authorization Act for Fiscal Year 2003. Public Law 107-314. 107th Cong., 2 December 2002.

Committee on National Security Systems Instruction (CNSSI) No. 4009. National Information Assurance (IA) Glossary. 26 April 2010.

Department of Defense Directive (DoDD) NUMBER 3200.11. *Major Range and Test Facility Base (MRTFB).* 27 December 2007.

Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) official web site. "Security Technical Implementation Guides (STIGs)." Accessed on 19 October 2015. http://iase.disa.mil/stigs/Pages/index.aspx

Department of Defense Instruction (DoDI) 8500.1. *Cybersecurity,* 14 March 2014.

Department of Defense Instruction (DoDI) 8510.01. *Risk Management Framework (RMF) for DoD Information Technology (IT),* 12 March 2014.

Department of Defense (DoD) 8570.01-M. *Information Assurance Workforce Improvement Program*, 24 January 2012.

Edwards, SES Terry G., Air Force Materiel Command A6/7, to ALHQCTR/CC/CL, ALHQSTAFF, ALINST/CC/CL. *Guidance on Approval of Obligation of Funds for Research, Development, Test and Evaluation (RDT&E), memorandum,* 11 Sep 2014.

Federal Bureau of Investigation official website. *Next Generation Identification: FBI Announces Biometric Suite's Full Operational Capability*. 23 September 2014.

Federal Information Security Management Act of 2002. Public Law 107-347. 107th Cong., 17 December 2002.

Fischer, Eric A., *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, Congressional Research Service, 20 June 2013.

Global Security website. *Military*. "Major Range and Test Facility Base [MRTFB]. accessed 10 October 2015, http://www.globalsecurity.org/military/facility/mrtfb.htm.

Grace, Thomas, Department of the Navy TAS Chief Engineer. Briefing. Subject: Telemetry of the Future. Date unknown.

*Information Technology Management Reform Act (ITMRA) of 1996 / Clinger-Cohen Act (CCA) of 1996.* Public Law 104-106. 104th Cong., 10 February 1996.

Kundra, Vivek, first United States Federal Chief Information Officer March 2009 through August 2011. *Memorandum for Chief Information Officers: Federal Data Center Consolidation Initiative*, 26 February 2010.

Maloney, Patrick, Enterprise Architect. *The Federal Data Center Consolidation Initiative (FDCCI): A plan to assist Federal agencies in meeting the goals and strategic objectives of the Federal Data Center Consolidation Initiative*. CA Technologies Solution white paper. August 2012.

*National Defense Authorization Act for Fiscal Year 2005*. Public Law 108-375, Cong., 108th. 28 October 2004.

*National Defense Authorization Act for Fiscal Year 2012*. Public Law 112-81, Cong., 112th. 31 December 2011.

National Institute of Standards and Technology (NIST) Special Publication 800-53. *Recommended Security Controls for Federal Information Systems*, February 2005.

Office of Management and Budget. *Fiscal Year 2009 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002.*

Office of Personnel Management official website. “Cybersecurity Resource Center.” accessed 26 September 2015, https://www.opm.gov/cybersecurity.

Putt, Archibald. *Putt’s Law and the Successful Technocrat: How to Win in the Information Age.* Wiley I-EEE Press, *April 2006.*

United States Government Accountability Office Report to Congressional Requestors, report GAO-14-713. *Data Center Consolidation: Reporting Can Be Improved to Reflect Substantial Planned Savings.* September 2014.

United States Government official website. “IT Dashboard FY2015 Edition.” https://itdashboard.gov/portfolios.

VanRoekel, Steven. Federal Chief Information Officer Memorandum. *Implementation Guidance for the Federal Data Center Consolidation Initiative (FDCCI).* Office of management and Budget Washington D.C., 19 March 2012.

## Table of Appendices

***Appendix A: Definition of Terms***

*Authorizing Official (AO)* – formally known as a Designated Approving Official (DAA). A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (CNSSI 4009).

*Cyber Tasking Order (CTO)* - An operational type order issued to perform specific actions at specific time frames in support of AF and Joint requirements. (AFI 10-1701)

*Data Center* – a closet, room, floor or building for the storage, management, and dissemination of data and information and [used to house] computer systems and associated components, such as database, application, and storage systems and data stores [excluding facilities exclusively devoted to communications and network equipment (e.g., telephone exchanges and telecommunications rooms)]. A data center generally includes redundant or backup power supplies, redundant data communications connections, environmental controls…and special security devices housed in leased, owned, collocated, or stand-alone facilities. (OMB)

*Defense Business Systems* - an information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. ( FY2005 NDAA)

*Effective and Economical* – For the purpose of this research "effective and economical" is defined by how capable current laws and policies are relative to RDT&E IT systems. In other words, if the intent of the laws and policies are able to be applied to RDT&E IT systems without perturbing their utility or purpose and if compliance cost (labor and money) are well below the procurement value and value of the function of the system the laws are then to be considered "effective and economical." However, if compliance requirements and costs exceed these thresholds then intent may have been lost and the laws and policies may not be "effective or economical." That is to say, if after bringing the system into compliance it is no longer capable of performing the function it was intended then the action was pointless. Moreover, if the cost of bringing the system into compliance exceed the initial cost of the system or the value the system brings to the mission then it is pointless as well.

*Enterprise Information Technology Data Repository (EITDR)* - The Air Force IT Portfolio Management system of record. EITDR is accessible through the Air Force Portal. EITDR contains a current inventory of initiatives, systems, and system-related data and is used

for internal management and oversight as well as to provide information to external sources to satisfy statutory and regulatory requirements. (AFI 33-141)

*Federal Data Center Consolidation Initiative (FDCCI)* - an Executive branch mandate from the Federal CIO that requires government agencies to reduce the overall energy and real estate footprint of their data centers, with the targeted goals of reduced costs, increased security, and improved efficiency. (Maloney)

*Information Assurance (IA)* - Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (CNSSI 4009)

*Installation Processing Node (IPN)* - A fixed DoD data center serving a single DoD installation and local area (installations physically or logically behind the network boundary) with local services that cannot (technically or economically) be provided from a CDC. There will be no more than one IPN per DoD installation but each IPN may have multiple enclaves to accommodate unique installation needs (e.g., Joint Bases). (AFI 33-115)

*Information Technology (IT)* - The term "information technology," with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.
(B) The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (ITMRA)

*Maintenance Tasking Order (MTO)* - Used by the AFCYBER community to assign workload to a field technician. (AFI 10-1701)

*Major Range and Test Facility Base (MRTFB)* - The designated core set of DoD Test and Evaluation (T&E) infrastructure and associated workforce that must be preserved as a national asset to provide T&E capabilities to support the DoD acquisition system. (DoDD 3200.11)

*Platform IT (PIT)* - IT, both hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. Examples of platforms that may include PIT are: weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical devices and health information technologies,

vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for industrial control systems including supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering, including associated data transport mechanisms (e.g., data links, dedicated networks). (DoDI 8500.01)

*Research, Development, Test, and Evaluation (RDT&E)* – associated efforts performed by installations to conduct research, develop, test, and evaluate weapon system capabilities and performance.

*Special Purpose Processing Node (SPPN)* - A fixed data center supporting special purpose functions that cannot (technically or economically) be supported by CDCs or IPNs due to association with infrastructure or equipment (e.g., communication and networking, manufacturing, training, education, meteorology, medical, modeling & simulation, test ranges, etc.). No general purpose processing or general purpose storage can be provided by or through a SPPN. SPPNs do not have direct connection to the Global Information Grid (GIG); they must connect through a CDC or IPN. (DoD CIO memorandum, "Department of Defense Joint Information Environment: Continental United States Core Data Centers and Application and System Migration," 11 July, 2013). (AFI 33-115)

*Special Purpose IT* – IT used for or dedicated to a single function aside from office automation functions. This type of IT function's more as a tool or monitoring device and may consist of a single computer or a group of networked computers.

*Security Technical Implementation Guides (STIG)* – configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. (DISA)

*Time Compliance Technical Order (TCNO)* - Directs a modification or change to a system or piece equipment and are published by the Program Management Office (PMO). (AFI 10-1701)